An evidence synthesis of strategies, enablers and barriers for keeping secrets online regarding the procurement and supply of illicit drugs

Grimani, Aikaterini; Gavine, Anna; Moncur, Wendy

Published in:
International Journal of Drug Policy

DOI:
10.1016/j.drugpo.2019.102621

Publication date:
2020

International Journal of Drug Policy 75 (2020) 102621

Contents lists available at ScienceDirect

International Journal of Drug Policy

journal homepage: www.elsevier.com/locate/drugpo

Review

An evidence synthesis of strategies, enablers and barriers for keeping secrets online regarding the procurement and supply of illicit drugs

Aikaterini Grimani[a,*], Anna Gavine[a], Wendy Moncur[a,b]

[a] School of Nursing and Health Sciences, University of Dundee, 11 Airlie Place, Dundee DD1 4HJ, United Kingdom
[b] Duncan of Jordanstone College of Art & Design, University of Dundee, 13 Perth Rd, Dundee DD1 4HT, United Kingdom

ARTICLE INFO

Keywords:
Illicit drug trade
Covert behaviours
Social networking sites
Digital technologies
Secrets
Internet

ABSTRACT

This systematic review attempts to understand how people keep secrets online, and in particular how people use the internet when engaging in covert behaviours and activities regarding the procurement and supply of illicit drugs. With the Internet and social media being part of everyday life for most people in western and non-western countries, there are ever-growing opportunities for individuals to engage in covert behaviours and activities online that may be considered illegal or unethical. A search strategy using Medical Subject Headings terms and relevant key words was developed. A comprehensive literature search of published and unpublished studies in electronic databases was conducted. Additional studies were identified from reference lists of previous studies and (systematic) reviews that had similar objectives as this search, and were included if they fulfilled our inclusion criteria. Two researchers independently screened abstracts and full-texts for study eligibility and evaluated the quality of included studies. Disagreements were resolved by a consensus procedure. The systematic review includes 33 qualitative studies and one cross-sectional study, published between 2006 and 2018. Five covert behaviours were identified: the use of communication channels; anonymity; visibility reduction; limited posts in public; following forum rules and recommendations. The same technologies that provide individuals with easy access to information, such as social networking sites and forums, digital devices, digital tools and services, also increase the prevalence of inaccurate information, loss of privacy, identity theft and disinhibited communication. This review takes a rigorous interdisciplinary approach to synthesising knowledge on the strategies adopted by people in keeping secrets online. Whilst the focus is on the procurement and supply of illicit drugs, this knowledge is transferrable to a range of contexts where people keep secrets online. It has particular significance for those who design online/social media applications, and for law enforcement and security agencies.

Introduction

This paper reports on an interdisciplinary systematic review conducted to uncover the covert strategies deployed by individuals engaged in illicit drug procurement and/or supply through online drug marketplaces and social media, and the enablers and barriers encountered in using these strategies. The research was carried out as part of the *Keeping Secrets Online* project (crestresearch.ac.uk/projects/keeping-secrets-online/), which synthesises new knowledge of how people use the Internet to facilitate secret-keeping in a range of contexts.

The topic of illicit drug procurement and supply was selected as a rich area of study as there is a high level of motivation for people to keep secrets in this context, due to the potential for punishment by the authorities and censure by family, colleagues and friends if caught. Drug offences are both severely punishable and highly stigmatised in the United Kingdom. For instance, possession of cannabis carries a sentence of up to five years in prison plus an unlimited fine, while its supply is punishable with up to 14 years in prison plus an unlimited fine (Askew & Salinas, 2019). Users and suppliers can be stigmatised or discriminated against irrespective of whether they have received a criminal record for their use. Thus sanctions for drug offences, which result in labelling and stigmatisation, can have long-term collateral consequences – e.g. convicted drug users/dealers may be subject to disapproval from their partners, friends or family, it may be more difficult for them to get a job, landlords may be reluctant to give them tenancies, and communities may resist the establishment of treatment centres where they can seek help (Askew & Salinas, 2019;

* Corresponding author.
E-mail address: grimaniaik@phs.uoa.gr (A. Grimani).

https://doi.org/10.1016/j.drugpo.2019.102621

Jones, Simonson, & Singleton, 2010).

The effects of certain drugs are considered to be sufficiently dangerous or harmful that their (nonmedical) use has been prohibited internationally. These drugs affect the Central Nervous System – either stimulating (e.g. (crack) cocaine or amphetamines or ecstasy) or inhibiting it (e.g. opiates, heroin or sedative-hypnotics such as benzodiazepines or barbiturates), – or cause hallucinogenic effects (such as marijuana or hashish, LSD, and phenocyclidine) (Houck & Siegel, 2015; Uutela, 2001). The secrets that need to be kept around their purchase and supply include who is involved, what is being traded, organisation of the delivery of drugs to physical locations, and financial transactions involved in buying and selling the drugs.

The Internet – and more broadly, digital technologies, devices and services – create considerable potential for online drug supply. The European Drug Report 2016 highlights the rapid rate of change in this area, driven by "increasing use of the internet, the deployment of new payment technologies, innovations in encryption and new options for the creation of distributed online marketplaces" (EMCDDA, 2016, p. 15). The challenges presented by these drivers "represent questions of critical importance for the future European policy agenda" (EMCDDA, 2016, p. 15). Here, we expand on each of these drivers – use of the internet, payment technologies, encryption and distributed online marketplaces – in turn, before considering opportunities for detecting illegal activity, and the overarching objectives of the systematic review undertaken.

Use of the Internet

Increasing use of the Internet for purchase and supply of drugs is seen both in terms of information and communications across multiple channels. i. Surface Web, Deep Web and Dark Web

Material contained within the Internet extends far beyond what is returned via standard search engines such as Google. Much is buried far down on dynamically generated sites, and standard search engines never find it (Bergman, 2001). The Internet can be understood as comprising of three elements: the Surface Web, Deep Web and Dark Web.

The *Surface Web* constitutes the part of the Web gathered and indexed by conventional general-purpose search engines such as Google, Firefox, Bing, etc. However, such search engines are capable of indexing just a small portion of available Web information (Beshiri & Susuri, 2019; EMCDDA & Europol, 2017; Iliou, Kalpakis, Tsikrika, Vrochidis, & Kompatsiaris, 2016).

Another part of the Internet is the *Deep Web* which comprises content that cannot be detected by the crawlers employed by conventional search engines, and includes information on the private networks and intranets that are password-protected behind logins, encrypted, or disallowed by the owner. By definition, private social media profiles on Facebook or Twitter are considered part of the Deep Web, too (Beshiri & Susuri, 2019; Iliou et al., 2016; Schäfer et al., 2019).

There is also a part of the Deep Web, known as the *Dark Web*, that provides anonymity both from a user and a data perspective, as its content is intentionally hidden and cannot be accessed by standard web browsers, but instead requires the use of special software. For this reason, the Dark Web has become popular for material such as "child pornography, unauthorised leaks of sensitive information, money laundering, copyright infringement, credit card fraud, identity theft, illegal sales of weapons and disseminating extremist content" (Weimann, 2016) The Dark Web is formed by several darknets such as The Onion Router (TOR) – which enables online anonymous communication – and the Invisible Internet Project (I2P), which is used for anonymous communication, users' traffic encryption, etc. (Beshiri & Susuri, 2019; EMCDDA & Europol, 2017; Iliou et al., 2016; Schäfer et al., 2019). The anonymity afforded by the Dark Web enables those engaged in the purchase and supply of drugs to conceal their identities. ii. Online communication via social media

The term "social media" serves as a blanket term for describing "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content" (Kaplan & Haenlein, 2010). Social media – notably social networking sites (SNS), forums and encrypted messaging services – act as central communication channels in the online supply and purchase of drugs.

In general terms, social media is an important part of internet use. It supports keeping in touch with friends and family, sharing photos and videos, staying up to date with news and current affairs – and maintaining communities of shared interest, whatever that interest may be. In the UK, 2018 data from OfCom shows extensive uptake of social media across society via the Surface Web – e.g. Facebook (88%), WhatsApp (61%), Instagram (38%), YouTube (35%), SnapChat and Twitter (25%) (OFcom, 2019). It is predictable that social media should be exploited for illegal activities. Indeed, social media – specifically *social networking sites* (SNS) – lend themselves to such activities, as "web-based services that allow individuals to construct a public or semi-public profile within a bounded system; articulate a list of other users with whom they share a connection; and view and traverse their list of connections and those made by others within the system" (Boyd & Ellison, 2007). Beneath the Surface Web, the Dark Web Social Network (DWSN) now offers a social networking site that is only accessible to Web browsers equipped with TOR, making it well-suited to the facilitation of drug purchase and supply as it provides assured anonymity (Gehl, 2016).

More broadly, *online forums* are the most common services appearing on the Dark Web. They serve as a disnormative space that enables illegal activities, within which drug dealers and users can articulate information needs and views around usage, availability and price of drugs (Haasio, Harviainen, & Savolainen, 2019). A further form of social media, *encrypted messaging services*, hold a key position within online drug markets. Increasingly, these services appear to be harnessed by vendors of illegal substances due to the lack of specialist knowledge required in their use, and provision of some security features that are expected to protect vendors from police detection and prosecution (Moyle, Childs, Coomber, & Barratt, 2019). Apps such as Kik, Wickr and WhatsApp that provide encrypted messaging services have become so central to drug supply that they present the "new way of online dealing". However, we emphasise that favoured forms of social media are subject to change, as online technologies evolve and new opportunities for unobserved communication surface.

Distributed online marketplaces: cryptomarkets

Drug markets have changed radically, with the internet increasingly used for the sale of drugs. As access to technology and the Internet has expanded noticeably, recent years have seen a dramatic growth in the sale of a variety of illicit substances via 'cryptomarkets' – hidden online marketplaces – with online sales projected to increase exponentially (Holt, 2017; Miller & Sønderlund, 2010; Mounteney, Oteo, & Griffiths, 2016). According to Martin (2014), cryptomarkets are anonymous online forums "*where goods and services are exchanged between parties who use digital encryption to conceal their identities*" (p. 356).

Cryptomarkets, and the cryptocurrencies – digital or virtual currencies that use cryptography for security – used to transact purchases on them, are central to the procurement and supply of illegal drugs, and intrinsically facilitate covert behaviour by buyer and seller (Aldridge & Décary-Hétu, 2016). An additional advantage of cryptomarkets is their association with substantially less threats and violence than conventional drug distribution channels such as friendships, dealers and open markets (Barratt, Ferris, & Winstock, 2016).

There are two essential elements that have given birth to cryptomarkets: anonymity networks and the use of anonymous financial transactions. Anonymity networks enable anonymous and untraceable access to the Internet. The Onion Router (TOR), is the most widely

adopted of these technologies (Gad, 2014). TOR was released in 2002. It is used to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis by directing Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays (Buxton & Bingham, 2015). Using TOR makes it more difficult for Internet activity to be traced back to the user, including their visits to websites, online posts, messages, and other communication forms (Gad, 2014). Further, to ensure their own privacy, users may encrypt their communications. The most common message encryption program is PGP (Pretty Good Privacy), used by cryptomarket administrators, vendors and buyers. PGP allows the user to encrypt text and files so that only the intended recipient is able to decrypt it (Mounteney et al., 2016).

The combination of covert communications and covert payments facilitated by TOR and message encryption programs has led to the proliferation of hidden web marketplaces. The most well-known cryptomarket was the “Silk Road” created in 2001, by Ross Ulbricht, who operated under the pseudonym of the Dread Pirate Roberts (Aldridge & Décary-Hétu, 2015). Silk Road was accessible only to people using TOR. Its main characteristics were the combination of technologies used to hide internet user activities and technologies that allowed individuals to make purchases with a digital, non-identity-carrying form of cash. Since its shutdown by the FBI in 2013, numerous other cryptomarkets have taken its place (Barratt & Aldridge, 2016; Foley, Karlsen, & Putniņš, 2019), and are used by cryptomarket traders.

Payment technologies: cryptocurrencies

Within cryptomarkets, traders use cryptocurrencies (Barratt, 2012) which enable anonymous financial transactions to both buyers and sellers. Cryptocurrencies are lines of computer code that hold monetary value, and are among the largest unregulated markets in the world (Gad, 2014; Maheshram & Singhai, 2018).

The first cryptocurrency (Bitcoin) was established in 2009 (Maurer, Nelms, & Swartz, 2013; Phelps & Watt, 2014). Bitcoin is a decentralised, peer-to-peer payment network that is powered by its users with no central authority or middle-men, using computational proof of the chronological order of transactions. The transactions are bundled together into a block which includes a cryptographic puzzle. The mathematics of the puzzle ensures that although it is difficult to solve, it is easy to verify. The system is secure and counterfeit-free as long as honest nodes control a majority of CPU power and thus it will become computationally impractical for an attacker to change the transactions (EMCDDA & Europol, 2017; Maurer et al., 2013; Nakamoto, 2008). It is an international currency, not associated with any country or central bank, backed only by its limited total supply and the willingness of Bitcoin users to recognise its value and trust its cryptographic algorithm (Maurer et al., 2013). The source code of Bitcoin was made freely available and therefore anyone can create a currency either identical to, or based on, the Bitcoin model. In the period between 2009 and 2014, many other cryptocurrencies have been established, such as Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin, Auroracoin, Vertcoin, MazaCoin, Coinye. However, there is limited information available about illegal activities involving Bitcoin, as well as the number of cryptocurrencies of all types that exist (Aldridge & Décary-Hétu, 2015; Foley et al., 2019; Maheshram & Singhai, 2018; Phelps & Watt, 2014; UNODC, 2014). It is known that the total market capitalisation of Bitcoin alone exceeds $250 billion as at January 2018, with a further $400 billion distributed across over 1,000 other cryptocurrencies (Foley et al., 2019).

Detecting illegal activity

Cryptocurrencies seem to be effective not only in facilitating illegal trade, but also in the detection of illegal activity despite the currency's anonymity, due to the public nature of the blockchain. For instance, monitoring transactions transmitted from computers to the blockchain enables individual transactions to be linked to the IP (Internet Protocol) address of the sender (Christin, 2013). Supporters of the anonymity provided by cryptocurrencies are developing new currencies that challenge such detection methods. These new currencies include Monero and ZCash, which both hide the user's identity (Foley et al., 2019).

In response to anonymity networks and the use of anonymous financial transactions, law enforcement agencies use a number of strategies to detect illegal activity on the hidden web, ranging from cyber-surveillance to forensic analysis. Such strategies include online detection by infiltrating the TOR network to determine individual IP addresses, and decoding the financial infrastructure of Bitcoin to identify individuals; postal detection and interception strategies by monitoring suspicious packages passing through the postal service, and ordering drugs on crypto markets to investigate the return address on the package; and online disruption by conducting major seizures (Christin, 2013; Foley et al., 2019; Kruithof et al., 2016).

There is a growing literature on the online illicit drug trade itself, yet limited empirical evidence exists concerning the related covert behaviours necessary to engage in this trade. This review therefore sought to understand what strategies people use to engage in covert illicit activities online, and how online technologies facilitate or obstruct illicit drug procurement and/or supply through online drug marketplaces and social media.

Objectives of the systematic review

The purpose of this systematic review was to (i) identify how people keep secrets online and what acts as enablers and barriers in the context of procurement/supply of illicit drugs, and (ii) identify how these strategies, enablers and barriers vary based on age, gender and culture. More specifically, the following research questions were addressed.

Research Question 1 (RQ1)

Strategies, enablers and barriers for keeping secrets online regarding procurement/supply of illicit drugs:

a) What strategies do people use to keep secrets online from family, friends and members of their wider social networks?
b) What enables effective implementation of the strategies identified in RQ1a?
c) What are the barriers to effective implementation of the strategies identified in RQ1a?

Research Question 2 (RQ2)

Effect of demographic variables on RQ1:

a) How are the strategies identified in RQ1 affected by age?
b) How are the strategies identified in RQ1 affected by gender?
c) How do strategies identified in RQ1 vary across non-western and diaspora populations?

Method

A systematic review of covert strategies, enablers and barriers regarding procurement/supply of illegal drugs was conducted. The protocol was registered in the International Prospective Register of Systematic Reviews (with Registration number CRD42018091687).

Inclusion criteria

Studies were included in the review if they met the following criteria:

Types of studies

Any quantitative or qualitative research study, which presented empirical methods and results, was considered for this review.

Types of participants

Any study conducted in western and non-western countries, with participants who engage in illegal drug procurement or supply, was included in this review. Studies focused on adolescents were excluded. No restrictions were placed on gender, geographical region, education level or sexuality.

Phenomenon of interest

The review includes studies which explored Internet use by individuals who are engaged in covert activities related to illegal drugs, and, more specifically, their procurement or supply.

Types of outcomes

The review was not restricted based on the kind of outcome studied, as the nature of the outcome measured was itself an item of interest. In particular, we were interested in covert behaviour strategies (i.e. financial transactions, network memberships, online drug forums, codewords), enablers and barriers. The secondary outcomes of our interest were the health effects from illegal drug use, as well as the effects of covert behaviour on physical and mental health (i.e. stress, quality of life).

Language

Only studies written in English language were included.

Date of publication

2004 – to current (searches conducted February 2018). The date was chosen considering the up-to-date technologies and the release year of networks of our interest. For example, Facebook was released on 2004, Myspace had been released one year earlier, while TOR had been released only 2 years earlier. Other social networking sites, such as Twitter, were released in later years.

Search strategy

A search strategy, using Medical Subject Headings (MeSH) terms and relevant key words was developed (Appendix Tables A and B). The MeSH is a controlled vocabulary for describing various topics which has been shown to greatly facilitate document retrieval. Many synonyms, near-synonyms, and closely related concepts are included as entry terms to help users find the most relevant MeSH descriptor for the concept they are seeking (Huang, Neveol, & Lu, 2011). The search strategies followed structured guidelines and standards used in social and health sciences (Higgins et al., 2011; Popay et al., 2006). This process facilitated a more evidence-based approach to literature searching, helped to rapidly and accurately locate the best available scientific information and avoided unnecessary searching. The search strategies included combining terms related to illicit drug use with terms related to internet use with Boolean operators. Searches were restricted to include studies published from 2004 until the date of the search (February 2018) and written in English language. No restrictions were placed on the search in terms of place of publication.

The following databases were searched: Medline (via Ovid), HMIC (via Ovid), ASSIA (via ProQuest), PsycInfo (Ebsco) and ACM Digital Library. In addition, Google Scholar was searched with the results being capped at the first 100 records (sorted by relevance). Grey literature was sought by manually searching the following websites relevant to the topic area: the CrimDoc (Criminology Library Grey Literature), the United Nations Office on Drugs and Crime, the National Crime Agency, RAND Co-operation, Interpol, and the PEW Research Centre. Editorials, letters, working papers, reports and reviews were excluded. Finally, in order to ensure no relevant studies were omitted, additional studies were identified from the reference lists of studies which met the inclusion criteria and were included in the review.

Study selection process

The screening process of abstracts and titles of all records identified by the search was conducted by two reviewers (AGr, AGa). The abstracts were included if they met the inclusion criteria or insufficient information was available in the abstract to determine eligibility. Any disagreements were resolved by AGr and AGa. The full text for any study that potentially met the inclusion was retrieved and independently screened by both AGr and AGa using a predesigned criteria form (Appendix Table C). Differences in judgment were resolved through a consensus procedure. A record was kept of all discarded full-text articles, including the reason for discard.

Quality assessment

Two review authors (AGr, AGa) independently evaluated the methodological quality of each study using an assessment tool appropriate to the study design. Discrepancies were resolved through a consensus procedure. Due to the methodological diversity of the included research studies, different assessment tools were used on a case by case basis. The Critical Appraisal Skills Program (CASP) Checklist for qualitative studies and the Appraisal tool for Cross-Sectional Studies (AXIS tool) were chosen.

The Critical Appraisal Skills Program (CASP) Checklist is an appraisal tool for qualitative studies which comprises 10 questions. The questions address three broad issues: (1) Are the results of the study valid? (2) What are the results? (3) Will the results help locally (how valuable is the research)? The CASP tool has areas to record a “yes”, “no” or “can't tell” answer for each question (Dixon-Woods et al., 2007; Walsh & Downe, 2006).

The following appraisal tool was developed for use in appraising observational cross-sectional studies. The Appraisal tool for Cross-Sectional Studies (AXIS tool) consists of 20 components. Seven (1, 4, 10, 11, 12, 16 and 18) of the questions related to quality of reporting, seven (2, 3, 5, 8, 17, 19 and 20) of the questions related to study design quality and six related to the possible introduction of biases in the study (6, 7, 9, 13, 14 and 15). The AXIS tool has areas to record a “yes”, “no” or “don't know” answer for each question and there is room for short comments as well. It has the benefit of providing the user the opportunity to assess each individual aspect of study design to give an overall assessment of the quality of the study. By providing this subjectivity, AXIS gives the user more flexibility in incorporating quality of reporting and risk of bias when making judgments on the quality of a paper (Downes, Brennan, Williams, & Dean, 2016).

Data extraction

A data extraction form was developed, reviewed and refined by the researchers to better capture the key aspects that are essential for evaluation, synthesis and presentation, ensuring the adequacy of the tool. The data extraction form includes information on publication (title, authors, year), aim of the study, country, context and setting, sampling approach, ethical issues, participant characteristics (e.g. number, age, gender), data collection methods (e.g. interview, focus group, questionnaire, lurking, web crawling), data analysis approach, data collected (e.g. number of interviews, number, number of forum posts), key themes. One reviewer extracted the data (AGr), while a

second reviewer (AGa) checked all the extracted data.

Evidence synthesis

A narrative synthesis of the findings from the included studies and the structures around the type of studies (experimental, survey, ethnography etc.) was provided. This approach is flexible, allowing for different types of evidence, qualitative and quantitative, to be reviewed (Mays, Pope, & Popay, 2005; Popay et al., 2006).

Content analysis was used to identify different clusters/groupings of strategies for secret keeping, the frequency with which these strategies are employed and the extent to which they are effective in maintaining privacy. Content analysis is a systematic, replicable technique for compressing many words of text into fewer content categories based on explicit rules of coding (Stemler, 2001). It is also useful for examining trends and patterns in documents (Mays et al., 2005; Popay et al., 2006). The process of creating codes was a combination of both predetermined (a priori) and emergent coding. Predetermined coding was based on a previous coding dictionary from other relevant research studies and key concepts, while emergent coding was based on concepts, actions, or meanings that evolved from the data and were different from the predetermined codes (Stemler, 2001).

Thematic analysis of the data, the most common method adopted within narrative reviews, was used to systematically identify the main, recurrent or most important themes or concepts across the included studies (Popay et al., 2006). Thematic analysis provides a means of organising and summarising the findings from large, diverse bodies of research (Mays et al., 2005; Popay et al., 2006). In order to identify the barriers and enablers which influence why a strategy may succeed or fail, the following three stages were conducted: coding text, developing descriptive themes, generating analytical themes (Thomas & Harden, 2008).

In addition, the qualitative software NVivo (12.0) was utilised to facilitate the conduct of the analysis. Using NVivo provides a robust and pragmatic way to manage the complexities of conducting qualitative evidence synthesis, facilitates framework synthesis and provides a clear audit trail, enhancing confidence in the synthesis findings (Houghton et al., 2017).

A process of translation of studies was used to explore the relationship between strategies used and the demographics. The robustness of the synthesis was also assessed by considering the quality of the evidence related to the research findings, for drawing conclusions about the strategies, facilitators and/or barriers identified in the synthesis. A summary discussion section was provided including the following: methodology of the synthesis used, evidence used, assumptions made, discrepancies and uncertainties identified (Popay et al., 2006).

Results

We first provide an overview of the studies returned by our systematic review. We then provide details of the covert strategies and associated facilitators and barriers identified within these studies, and assess the quality of the included studies.

Literature searches

Our primary search in the predefined databases resulted in 1198 hits. A further 225 hits were found in other sources, giving a total of 1423 citations (see Fig. 1). The latter included references from relevant studies and reviews, publications from the CrimDoc: Criminal Justice Grey Literature Database and Google scholar. After duplicates were removed ($n=70$), a total of 1353 citations were screened against the inclusion criteria. Of these, 1273 citations were excluded on the basis of title, keywords, and abstract. The full texts of the remaining articles ($n=80$) were then assessed against the inclusion criteria, resulting in 34 articles being retained. The reasons for exclusion are presented in Fig. 1.

Description and characteristics of included studies

Thirty-four studies were identified that focused on procurement/supply of illegal drugs, published between 2006 and 2018. Thirty-three were qualitative studies and one was a cross-sectional study. Data sources were mainly obtained from vendor listings, threads, forum posts, tweets and encrypted online interviews. The studies were conducted in the following countries: USA ($n=1$), Australia ($n=4$), Canada ($n=1$), Ireland ($n=3$), Germany ($n=1$), Finland ($n=1$), Switzerland ($n=1$), Multi-country ($n=9$), N/A ($n=13$). An overall description of the included studies and details of the study designs are presented in Supplementary Table 1.

Each of the studies included a diverse range of strategies, facilitators and/or barriers. Five covert strategies related to illegal drug trade were identified (see Table 2a): (1) use of communication channels; (2) anonymity, such as anonymous web browsing; (3) visibility reduction; (4) limited posts in public; (5) following forum rules and recommendations. The same digital tools and services that provide individuals with easy access to information and enable illegal drug trade-related behaviours, were also used to deter these behaviours (see Tables 3a and 4a).

A summary of strategies, facilitators and barriers is provided below. Supplementary Table 2b presents fuller descriptions of the strategies of the included studies. Supplementary Tables 3b and 4b present fuller description of the facilitators and barriers of the included studies.

Covert strategies

Use of communication channels

Eight studies reported digital use of communication channels as a covert strategy related to procurement/supply of illegal drugs. Members of the Deep Web drug forums leverage censorship-resistant communication tools like TOR (The Onion Router) to access an encrypted Internet environment where their ideas can be exchanged freely and their need for illicit drugs can be met securely (Backman, 2013). For example, cryptomarket forums, such as Merkat, have become meeting points where different kinds of knowledge can be combined and validated. They develop a risk infrastructure that provides technical tools, shared knowledge, and shareable judgements to manage risk (Bancroft, 2017). Moreover, the deep web Reddit website serves as a social space, where multiple different sub-contexts operate together and form a grand context for information transfer among people (Costello, Martin, & Edwards Brinegar, 2017). In addition, when considering Internet use (a web site, electronic chat room, or e-mail) to obtain drugs or reach a drug dealer, (Gordon, Forman, & Siatkowski, 2006). Barratt (2011) indicated that almost one third of participants used private online communication modes to discuss drugs. These private modes included instant messaging, private messaging and non-public-access forums. Twitter also represents a viable modality for criminal actors to engage in the illegal marketing and sale of prescription-controlled substances online (Mackey & Kalyanam, 2017; Mackey, Kalyanam, Katsuki, & Lanckriet, 2017). Lavorgna (2015) highlighted the role of the Internet as an enhanced communication tool among actors involved in illegal businesses, allowing newcomers to interject themselves in the trafficking chain as local or even international retailers. Communication generally occurs, for instance, via email spam and online pharmacies, so that in most cases it is unidirectional from the seller to the buyer. Furthermore, Barratt, Allen, and Lenton (2014) presented the case of 'Australian Bluelight' drug forum moderators, who used e-mail to warn other ecstasy users on their forum about the dangers of inadvertently using PMA (para-methoxyamphetamine), after the death of 20-year-old Annabel Catt from this drug.

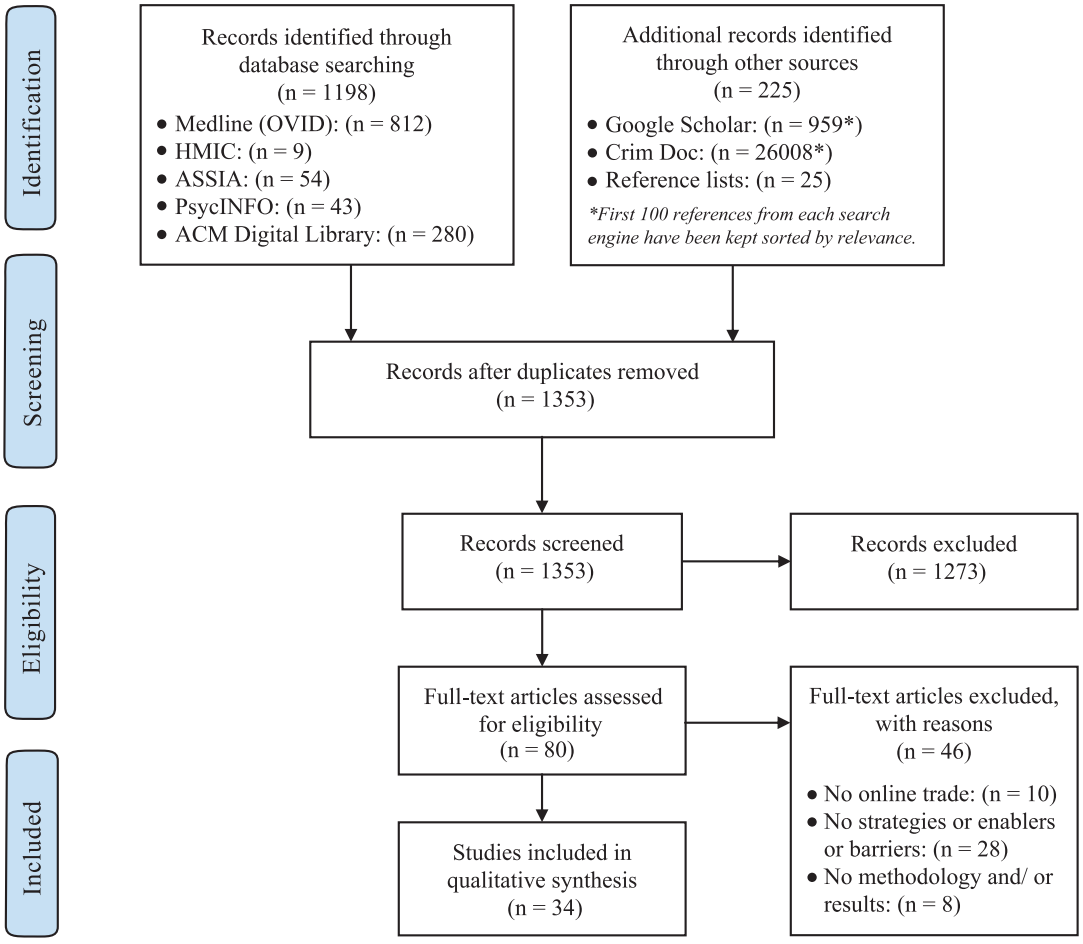

Fig. 1. Flow chart of the study selection process used for the systematic review.

Table 2a
Covert strategies related to illegal drug trade.

Strategies	No of studies and references	
Use of communication channels	8	(Backman, 2013; Barratt, 2011; Barratt et al., 2014; Costello et al., 2017; Gordon et al., 2006; Lavorgna, 2015; Mackey & Kalyanam, 2017; Mackey et al., 2017)
Anonymity/ghost accounts	29	(Aldridge & Askew, 2017; Aldridge & Décary-Hétu, 2014, 2016; Backman, 2013; Bancroft, 2017; Bancroft & Scott Reid, 2017; Barratt, 2011; Barratt, Lenton, Maddox, & Allen, 2016; Broseus et al., 2017; Broséus et al., 2016; Costello et al., 2017; Dolliver, 2015; Duxbury & Haynie, 2018; Hall et al., 2017; Hardy & Norgaard, 2016; Holt et al., 2015; Maddox et al., 2016; Moeller et al., 2017; Morselli et al., 2017; Nurmi et al., 2017; Paquet-Clouston et al., 2018; Phelps & Watt, 2014; Rhumorbarbe et al., 2016; Soska & Christin, 2015; Tzanetakis et al., 2016; van de Ven & Koenraadt, 2017; Van Hout & Bingham, 2013a, 2013b; Van Hout & Bingham, 2014)
Visibility reduction	3	(Aldridge & Askew, 2017; Barratt, 2011; Costello et al., 2017)
Limited posts in public	2	(Backman, 2013; Barratt, 2011)
Following forum rules and recommendations	3	(Backman, 2013; Barratt, 2011; Phelps & Watt, 2014)

Table 3a
Technology which enables illegal drug trade-related behaviours.

Facilitators	No of studies and references	
Social networking sites/forums	9	(Backman, 2013; Barratt, 2011; Barratt et al., 2014; Holt et al., 2015; Lavorgna, 2015; Mackey & Kalyanam, 2017; Mackey et al., 2017; Maddox et al., 2016; Phelps & Watt, 2014)
Digital devices	1	(Gordon et al., 2006)
Digital tools and services	26	(Aldridge & Askew, 2017; Aldridge & Décary-Hétu, 2014, 2016; Backman, 2013; Bancroft, 2017; Bancroft & Scott Reid, 2017; Barratt, 2011; Barratt et al., 2016; Broseus et al., 2017; Broséus et al., 2016; Dolliver, 2015; Duxbury & Haynie, 2018; Hall et al., 2017; Hardy & Norgaard, 2016; Holt, 2017; Lavorgna, 2015; Maddox et al., 2016; Nurmi et al., 2017; Phelps & Watt, 2014; Rhumorbarbe et al., 2016; Soska & Christin, 2015; Tzanetakis et al., 2016; van de Ven & Koenraadt, 2017; Van Hout & Bingham, 2013a, 2013b; Van Hout & Bingham, 2014)

Table 4a
Technology which deters illegal drug trade-related behaviours.

Barriers	No of studies and references	
Social networking sites/forums	2	(Costello et al., 2017; Moeller et al., 2017)
Digital tools and services	4	(Bancroft & Scott Reid, 2017; Moeller et al., 2017; Morselli et al., 2017; Paquet-Clouston et al., 2018)

Anonymity/ghost accounts

Twenty-nine studies reported anonymity as a covert strategy related to procurement/supply of illegal drugs. Cryptomarkets enable buyers and sellers to transact with a considerable degree of anonymity by virtue of their location on the hidden web, making it difficult for law enforcement to trace marketplace activity to participants. These online markets use (i) the virtually untraceable cryptocurrency Bitcoin, (ii) The Onion Router (TOR) service and (iii) the encryption of private messages, files and e-mails using the Pretty Good Privacy (PGP) cryptosystem to ensure anonymity (Broséus et al., 2016). Although they are not completely anonymous, the use of cryptocurrencies like Bitcoin obfuscate links between payments and individuals, particularly when combined with recent developments like bitcoin tumblers that further obscure payment trails (Aldridge & Askew, 2017; Bancroft & Scott Reid, 2017). According to Barratt (2011), avoiding the sharing of identifying information online, such as the full name and suburb, as well as the names and contact details of friends and dealers, was a commonly mentioned strategy. In addition, some of the participants used one or more pseudonyms online, which were sometimes linked to their 'real life' identities, in order to reduce the risks of disclosing their identity via online drug discussions. The use of guest/anonymous accounts and browsing protection tools like TOR were also described as anonymity strategies. In particular, the use of anonymisation services like TOR in combination with the following cryptomarkets was described: Silk Road (Aldridge & Décary-Hétu, 2014; Barratt & Aldridge, 2016; Hardy & Norgaard, 2016; Maddox, Barratt, Allen, & Lenton, 2016; Mounteney et al., 2016; Nurmi, Kaskela, Perälä, & Oksanen, 2017; Phelps & Watt, 2014; Van Hout & Bingham, 2013a, 2013b; Van Hout & Bingham, 2014), Silk Road 2 (Broseus, Morelato, Tahtouh, & Roux, 2017; Broséus et al., 2016; Dolliver, 2015), Cryptomarket (Duxbury & Haynie, 2018), Alphabay (Paquet-Clouston, Décary-Hétu, & Morselli, 2018), Evolution (Broseus et al., 2017, 2016; Rhumorbarbe, Staehli, Broseus, Rossy, & Esseiva, 2016), and Agora (Broséus et al., 2016; Soska & Christin, 2015; Tzanetakis, Kamphausen, Werse, & von Laufenberg, 2016). Furthermore, several studies described the use of cryptocurrency, like Bitcoin, for transactions (Aldridge & Décary-Hétu, 2016; Backman, 2013; Bancroft, 2017; Bancroft & Scott Reid, 2017; Maddox et al., 2016; Moeller, Munksgaard, & Demant, 2017; Morselli, Décary-Hétu, Paquet-Clouston, & Aldridge, 2017; Phelps & Watt, 2014; Rhumorbarbe et al., 2016; Soska & Christin, 2015; Tzanetakis et al., 2016; Van Hout & Bingham, 2013a, 2013b). Another common anonymity strategy that has been described is the use of encrypted communication, such as Pretty Good Privacy (PGP) or Privnote (Aldridge & Askew, 2017; Backman, 2013; Bancroft & Scott Reid, 2017; Broséus et al., 2016; Soska & Christin, 2015). Additional anonymity strategies are:

- the destruction of evidence as soon as it's feasible (Aldridge & Askew, 2017);
- the extension of the users' technical knowledge and skills in order to understand how the online illicit drug market works and how to hide their IP address (Bancroft & Scott Reid, 2017);
- attestability of a persona, as well-known vendors would establish themselves across different markets (Bancroft & Scott Reid, 2017);
- deniability – i.e. using a false name for deliveries and scrubbing stored addresses (Bancroft & Scott Reid, 2017);
- masking personal identifiers – i.e. users would avoid using a picture of themselves (Costello et al., 2017);
- the use of websites such as online pharmacies, business-to-business websites, social media websites (Hall, Koenraadt, & Antonopoulos, 2017);
- the use of electronic payment systems, providing a modicum of privacy and anonymity (Holt, Smirnova, Chua, & Copes, 2015);
- using ghost websites (advertise goods and take money, but usually have no intention of delivering a product of good quality) to market IPED (image and performance enhancing drugs) market (van de Ven & Koenraadt, 2017).

Visibility reduction

Three studies reported visibility reduction as a covert strategy related to procurement/supply of illegal drugs. Barratt (2011) implied that forum users attempted to reduce the risks of drug discussion in public online forums by reducing self-incrimination. It was considered to be less dangerous to describe past experiences of drug use than dealing and supply, or than referring to present or future drug use. Others used vague language, code words and the third person to describe their own experiences, notably by using the acronym SWIM (*Someone Who Isn't Me*). An additional forum user mentioned avoiding risk when posting images of drugs by photographing small amounts of drugs, and excluding any identifying information from the image. Likewise, Costello et al. (2017) reported the use of coded language - e.g. participants called marijuana "pizza" – and the acronym SWIM. Other visibility reduction strategies according to Aldridge and Askew (2017) were the following:

- vetting potential customers who may risk drawing mainstream attention to the marketplace;
- providing real, rather than fake, names (to reduce the chances of shipment interception);
- selecting delivery drop-off locations at a distance from home or work;
- reducing the visibility of routine activities by rotating drop-off points;
- avoiding entering post offices where they might be recorded by CCTV;
- disrupting routines involved in offline activities to make these less visible;
- making more visible the 'ordinary' routine activities in receiving 'legitimate' deliveries;
- small quantities of shipping drugs to appear as ordinary business letters;
- "stealth" packaging (disguise suspect contents to reduce the visibility of cryptomarket vendor activities).

Limited posts in public

Two studies reported limited posts in public as a covert strategy related to procurement/supply of illegal drugs. According to Backman (2013), forum users posted or left a comment on the forums only if necessary. Barratt (2011) indicated that forum users described reducing risks by both avoiding drug discussion in public internet forums, and by participating in such discussion in less risky ways, for example by discussing drugs infrequently.

Following forum rules and recommendations

Three studies reported following forum rules and recommendations as a covert strategy related to procurement/supply of illegal drugs. For

example, Backman (2013) included a number of behaviour recommendations that members believed would help the community in avoiding arrests. In addition, user advice concerning security correlated with technology and Bitcoins had always been a common normative order in the deep Web drug forums. The findings of Barratt (2011) showed that some of the forum users, who engaged in some drug discussion in public online forums attempted to reduce the risks of these discussions by following the forum drug discussion rules. A popular video sharing website also featured videos on users' advice, recommendations and perspectives of Silk Road (Phelps & Watt, 2014).

Facilitators of covert strategies

Social networking sites/forums

Nine studies reported social networking sites as an effective facilitator of covert strategies related to procurement/supply of illegal drugs. Drug cryptomarkets function as communities that enable information sharing for reducing the risks posed by law enforcement to illegal drug trading (Aldridge & Askew, 2017). For example, Barratt (2011) implied that most of those who avoided drug discussion in public forums used private online communication modes, such as instant messaging, private messaging and non-public-access forums. Specifically, use of instant messaging protocols is popular amongst the Russian hacker community (Holt et al., 2015). Bluelight.ru drug forum used e-mail to warn other ecstasy users about the dangers of inadvertently using PMA (Barratt et al., 2014). According to Lavorgna (2015) Internet networks have facilitated communication, enhanced efficiency and have also changed the internal organisation of criminal networks. Mackey and Kalyanam (2017) and Mackey et al. (2017) showed Twitter as the catalyst for online promotion of illicit substances such as fentanyl. Deep web cryptomarkets, such *as BlackMarket Reloaded* and *Sheep Marketplace* used multiple communication approaches in order to determine who to trust (Backman, 2013). In addition, Silk Road forums facilitated an openness towards discussion of illicit behaviour, covering topics including how to use Silk Road and the dangers of taking illicit drugs and anonymity, while the Silk Road Wiki page offered advice and assisted users with understanding the basic principles of anonymity (Maddox et al., 2016; Phelps & Watt, 2014).

Digital devices

One study reported digital devices as an effective facilitator of covert strategies related to procurement/supply of illegal drugs. In particular, according to Gordon et al. (2006), a high proportion of the sample had access to a computer with an internet connection and mobile telephone.

Digital tools and services

Twenty-six studies reported digital tools and services as an effective facilitator of covert strategies. For example, Barratt (2011) indicated that few forum users used TOR (browsing protection tool) and guest/anonymous accounts to prevent authorities from potentially identifying them through tracking their IP address. Cryptomarkets are online venues that allow drug vendors to span broad audiences, reshape organisational structure, and remain relatively anonymous and include the following platforms: Silk Road (Aldridge & Décary-Hétu, 2014, 2016; Barratt & Aldridge, 2016; Hardy & Norgaard, 2016; Nurmi et al., 2017; Van Hout & Bingham, 2013a, 2013b; Van Hout & Bingham, 2014), Silk Road 2 (Broseus et al., 2017; Dolliver, 2015), Cryptomarket (Duxbury & Haynie, 2018), Merkat (Bancroft & Scott Reid, 2017), Evolution (Broseus et al., 2017; Rhumorbarbe et al., 2016) and Agora (Soska & Christin, 2015; Tzanetakis et al., 2016). The key recommendation by Deep Web users was the use of encrypted communication, via PGP. However, this good practice was not always followed (Aldridge & Askew, 2017; Backman, 2013; Bancroft & Scott Reid, 2017; Broséus et al., 2016; Soska & Christin, 2015). Various online sites and payment facilities are simultaneously used to sell illicit drugs (Hall et al., 2017). For example, the online IPED market (Image and Performance Enhancing Drugs) earned positive comments from most online buyers' experiences (van de Ven & Koenraadt, 2017). In addition, social engineering is a common tool in many internet-mediating trafficking activities, such as online illicit drug trade (Lavorgna, 2015). Electronic payment systems provide a modicum of privacy and anonymity for the participants (Holt et al., 2015). Escrow was a service offered by Silk Road administrators, to protect sellers and buyers from fraud, offering a level of security in their transactions. The service allowed the bitcoins to be stored by Silk Road until the buyer received their product (Aldridge & Décary-Hétu, 2016; Backman, 2013; Bancroft, 2017; Bancroft & Scott Reid, 2017; Maddox et al., 2016; Phelps & Watt, 2014; Rhumorbarbe et al., 2016; Soska & Christin, 2015; Tzanetakis et al., 2016; Van Hout & Bingham, 2013a, 2013b).

Barriers to the use of covert strategies

Social networking sites/forums

Two studies reported social networking sites as an effective barrier to covert strategies related to procurement/supply of illegal drugs. According to Costello et al. (2017) banter facilitates disclosure of elicit behaviours in subreddits. In addition, the reputation system creates a type of fraudulent resource exchange that revolves around unreliable feedback and fake accounts (Moeller et al., 2017).

Digital tools and services

Four studies reported digital tools and services as an effective barrier of covert strategies related to procurement/supply of illegal drugs. For example, multiple identities are a challenge for users and vendors. Having several identities in the same market was thought to be suspicious and the act of scammers, fake vendors and hostile vendors producing critical or insulting comments about rival vendors (Bancroft & Scott Reid, 2017). In addition, some vendors make threats of doxing (when a person's anonymous online persona is linked with their real-world identity and address) (Bancroft & Scott Reid, 2017; Morselli et al., 2017). However, vendors still need to gain knowledge of how the marketplace and the technologies related to it work in order to successfully conceal their identity. Moreover, they need to learn how to successfully conceal and ship the product without attracting attention from law enforcement agencies, while barriers to sales may be due to buyers' tendencies to avoid the risks of transaction failures in online markets, and to opt for safer and reputable suppliers (Paquet-Clouston et al., 2018). In addition, cryptomarkets are targeted at the system level by Denial of Service (DoS) attacks and hacking. Several sites have publicised statements of being victims of DoS attacks, as well as hacks and subsequent theft. These attacks consist of gaining access to databases with information on incriminating and illegal acts, which may include unencrypted addresses of inexperienced users and bitcoins. The irreversibility of transactions, and the pseudonymous and anonymisable properties makes bitcoin a perfect target for heists (Moeller et al., 2017).

Quality assessment

The overview of quality assessment of the 33 qualitative studies is summarised in Supplementary Table 5. The majority of the studies stated the aims of the research clearly ($n = 27$), used appropriate qualitative methodology ($n = 30$) and recruitment strategy ($n = 28$) and collected the data in a way that addressed the research issues ($n = 27$). In addition, they included sufficiently rigorous data analysis ($n = 23$), stated the findings clearly ($n = 21$), as well as discussing the contribution of the study and the generalisability of research findings ($n = 29$). Almost half of the studies used the appropriate research design to address the aims of the research. For the majority of the studies, neither the relationship between researcher and participants has been

adequately considered ($n = 30$) nor the ethical issues have been taken into consideration ($n = 15$).

The quality assessment of the cross-sectional study (Duxbury & Haynie, 2018) is detailed in Supplementary Table 6. In summary, the study fulfils the majority of the questions. However, there are some limitations regarding the response rate, the limitations of the study and the ethical approval or consent of the participants. Nonresponse bias occurs if the non-responders are substantially different to the rest of the population in the sample. Thus, any information on non-responders is crucial. In addition, if the issue of limitations is not explored, this is cause for concern that the limitations don't stop at the design and that the researcher(s) has a poor understanding of the study as a whole.

Discussion

Main findings

This review sought to understand how people use the internet when engaging in covert activities regarding procurement/supply of illicit drugs. A total of 34 studies (33 qualitative studies and one cross-sectional study) were included in the evidence synthesis. Notably, with the exception of one study published in 2006, all other studies were published from 2011 onwards.

Strategies, enablers and barriers for keeping secrets online

Five covert strategies were identified:

- use of communication channels; anonymity (i.e. anonymous web browsing);
- anonymity/ghost accounts;
- visibility reduction (i.e. coded language);
- limited posts in public (i.e. avoiding drug discussion in public);
- following forum rules and recommendations.

The same digital tools and services that provide individuals with easy access to information and enable illegal drug trade-related behaviours, were also used to deter these behaviours. In particular, social networking sites were identified as effective facilitators of covert strategies. For example, Deep Web forums facilitated an openness for discussion of illicit behaviours. Digital devices (i.e. computers, cell phones, and smartphones), as well as digital tools and services were also identified as effective facilitators of covert strategies. For example, cryptomarkets, cryptocurrency and encrypted communication facilitate illicit drug trades. Conversely, social networking sites, as well as digital tools and services were identified as effective barrier of covert strategies.

No secondary outcomes such as effects on physical and mental health due to covert behaviour were reported in the included studies.

Effect of demographic variables on identified strategies

Due to the sensitive topic of the review, the majority of the included studies lacked adequate information about demographic characteristics, such as gender, age and geographical region. However, this was anticipated, as anonymity enables internet users to hide their identity with regard to demographic information and personality, and to violate the law whilst evading detection. It was therefore difficult to explore the relationship between strategies used and the demographics, and to draw general conclusions. The studies included data which were mainly obtained from vendor listings, threads, forum posts, tweets and encrypted online interviews. Thus, none of the studies included information about the effect of age, gender and geographical region on identified strategies. Therefore, more research is needed on scientifically assured methods for measuring and analysing targeted outcomes, in relation to demographic characteristics.

Strengths and limitations

One of the strengths of this literature review is the use of an interdisciplinary approach which utilised robust methods of evidence synthesis developed in the field of health sciences and drew on literature from computing, criminology and health. The methodological approach ensured that a comprehensive search strategy was used, and this facilitated a more evidence-based approach to literature searching in the field of human–computer interaction where this is not standard practice. Moreover, inclusion of study designs other than quantitative studies gave a wide and diverse range of evidence. In the present systematic review, we also included "grey" literature from western and non-western countries.

Another important strength is the use of diverse methodological quality assessment tools, to assess the risk of bias of the included qualitative, quantitative and mixed-methods studies. Due to the nature of the evidence sought, it was difficult to pre-define and include them in the search strategy, which may lead to the exclusion of some studies from the review. In addition, studies not in English were excluded from the study, which may bias the findings.

We acknowledge the limitations regarding the number of studies, the diverse nature of the strategies, the number of targeted outcomes regarding facilitators and barriers, the methodological quality of studies included, and the insufficient reporting of evidence. As such, the results should be interpreted with some caution.

Generalisability of findings

In this paper, we have focussed on the strategies, enablers and barriers involved in keeping secrets online regarding the procurement and supply of illicit drugs. The study was carried out as part of a larger project, *Keeping Secrets Online* [ref https://crestresearch.ac.uk/projects/keeping-secrets-online/], which also examines secret-keeping in two further contexts: intimate partner violence (Grimani, Gavine, & Moncur, 2019a) and infidelity (Grimani, Gavine, & Moncur, 2019b).

The *Keeping Secrets Online* project synthesises new knowledge that is intended to be useful to those who support people keeping secrets legitimately as part of their job, and will enhance the UK's capacity to detect and mitigate threats generated via online channels. Findings on illicit drugs reported herein were distilled and presented within a specially commissioned book, the 'Illustrated Guide to Keeping Secrets Online' (Moncur et al., 2019), along with findings form the other two contexts. The Guide summarises research findings in an easy-to-read format, made up of narratives supported by illustrations and research insights. It has been used to stimulate fruitful discussion with key stakeholders, generating further knowledge on how the strategies, barriers and enablers uncovered by our research can be applied to people who need to keep secrets as part of their jobs in countering UK and international security threats.

Conclusion and implications

The rapid rate of change in how illicit drugs are purchased and supplied via online channels, digital technologies, devices and services presents challenges of critical importance for policy agendas (EMCDDA, 2016). Through this systematic review, we provide insights into the covert behaviour strategies associated with the supply and purchase of illicit drugs online. These strategies were enabled through easy access to information online, and by digital devices, tools and services. However, they were also subject to barriers, with risks emanating from inaccurate information, loss of privacy, identity theft and disinhibited communication.

The review highlights the need for more well-designed studies that address strategies for online secret-keeping, and more scientifically assured methods for measuring and analysing targeted outcomes in relation to demographic characteristics. There was also a gap in the

research regarding the effects on physical and mental health outcomes due to online covert behaviours and activities.

The insights provided in this review may support policymakers in considering how best to respond to the emergent challenges on online purchase and supply of illicit drugs, and to exploit the opportunities that online channels offer for reducing drug problems. Further, through our approach to generalisation of findings, the synthesised knowledge is already helping law enforcement and security agencies to develop the UK's capacity to support people who keep secrets as part of their jobs, and who work to detect and mitigate threats generated via online channels.

Funding

This work was supported by the Centre for Research and Evidence on Security Threats.

Conflict of Interest Statement

The authors confirm that there are no known conflicts of interest associated with this publication.

CRediT authorship contribution statement

Aikaterini Grimani: Data curation, Methodology, Writing - original draft, Writing - review & editing. **Anna Gavine:** Data curation, Methodology, Writing - review & editing. **Wendy Moncur:** Supervision, Writing - review & editing.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.drugpo.2019.102621.

References

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *The International Journal of Drug Policy, 41*, 101–109.

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation.* SSRN.

Aldridge, J., & Décary-Hétu, D. (2015). *Cryptomarkets: The darknet as an online drug market innovation.* NESTA.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *The International Journal of Drug Policy, 35*, 7–15.

Askew, R., & Salinas, M. (2019). Status, stigma and stereotype: How drug takers and drug suppliers avoid negative labelling by virtue of their 'conventional' and 'law-abiding' lives. *Criminology & Criminal Justice, 19*(3), 311–327.

Backman, B. (2013). *Follow the white rabbit: An ethnographic exploration into the drug culture concealed within the "deep Web".* University of Nebraska at Omaha.

Bancroft, A. (2017). Responsible use to responsible harm: illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk & Society, 19*(7–8), 336–350.

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society, 20*(4), 497–512.

Barratt, M. J. (2011). Discussing illicit drugs in public internet forums: visibility, stigma, and pseudonymity. *Proceedings of the 5th international conference on communities and technologies*.

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction, 107*(3), 683.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy, 35*, 1–6.

Barratt, M. J., Allen, M., & Lenton, S. (2014). "PMA sounds fun": Negotiating drug discourses online. *Substance Use & Misuse, 49*(8), 987–998.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy, 35*, 24–31.

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016). 'What if you live on top of a bakery and you like cakes?' Drug use and harm trajectories before, during and after the emergence of Silk Road. *The International Journal of Drug Policy, 35*, 50.

Bergman, M. K. (2001). White paper: The deep web: Surfacing hidden value. *Journal of electronic publishing, 7*(1), https://doi.org/10.3998/3336451.0007.104.

Beshiri, A. S., & Susuri, A. (2019). Dark web and its impact in online anonymity and privacy: A critical analysis and review. *Journal of Computer Communications, 7*(3), 30–43.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230.

Broseus, J., Morelato, M., Tahtouh, M., & Roux, C. (2017). Forensic drug intelligence and the rise of cryptomarkets. Part I: Studying the Australian virtual market, 279, 288-301.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International, 264*, 7–14.

Buxton, J., & Bingham, T. (2015). *The rise and challenge of dark net drug markets*. Retrieved from https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd international conference on world wide web*.

Costello, K. L., Martin, J. D., & Edwards Brinegar, A. (2017). Online disclosure of illicit information: Information behaviors in two drug forums. *Journal of the Association for Information Science and Technology, 68*(10), 2439–2448.

Dixon-Woods, M., Sutton, A., Shaw, R., Miller, T., Smith, J., Young, B., et al. (2007). Appraising qualitative research for inclusion in systematic reviews: a quantitative and qualitative comparison of three methods. *J Health Serv Res Policy, 12*(1), 42–47.

Dolliver, D. S. (2015). Evaluating drug trafficking on the tor network: Silk Road 2, the sequel. *International Journal of Drug Policy, 26*(11), 1113–1123.

Downes, M. J., Brennan, M. L., Williams, H. C., & Dean, R. S. (2016). Development of a critical appraisal tool to assess the quality of cross-sectional studies (AXIS). *BMJ Open, 6*(12), e011458.

Duxbury, S. W., & Haynie, D. L. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks, 52*, 238–250.

EMCDDA. (2016). *European drug report 2016: Trends and developments.* Luxembourg: Publications Office of the European Union.

EMCDDA, & Europol. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Luxembourg: EMCDDA–Europol Joint publications, Publications Office of the European Union.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853.

Gad, M. (2014). Crimeware marketplaces and their facilitating technologies. *Technology Innovation Management Review, 4*(11), 28–33.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 18*(7), 1219–1235.

Gordon, S. M., Forman, R. F., & Siatkowski, C. (2006). Knowledge and use of the internet as a source of controlled substances. *Journal of Substance Abuse Treatment, 30*(3), 271–274.

Grimani, A., Gavine, A., & Moncur, W. (2019). *An evidence synthesis of covert strategies, enablers and barriers for keeping secrets online regarding intimate partner violence* (Submitted)University of Dundee.

Grimani, A., Gavine, A., & Moncur, W. (2019). *An evidence synthesis of secretive behaviour strategies, enablers and barriers for keeping secrets online regarding infidelity* (Submitted) University of Dundee.

Haasio, A., Harviainen, J. T., & Savolainen, R. (2019). Information needs of drug users on a local dark Web marketplace. *Information Processing & Management* https://doi.org/10.1016/j.ipm.2019.102080.

Hall, A., Koenraadt, R., & Antonopoulos, G. A. (2017). Illicit pharmaceutical networks in Europe: Organising the illicit medicine market in the United Kingdom and the Netherlands. *Trends in Organized Crime, 20*(3–4), 296–315.

Hardy, R. A., & Norgaard, J. R. (2016). Reputation in the Internet black market: An empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics, 12*(3), 515–539.

Higgins, J. P., Altman, D. G., Gotzsche, P. C., Juni, P., Moher, D., Oxman, A. D., et al. (2011). The Cochrane Collaboration's tool for assessing risk of bias in randomised trials. *BMJ, 343*, d5928.

Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime, 18*(1), 1–10.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime, 16*(2), 81–103.

Houck, M. M., & Siegel, J. A. (2015). *Illicit drugsFundamentals of Forensic Science* (3rd ed.). Oxford: Academic Press315–352.

Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2017). From screening to synthesis: using nvivo to enhance transparency in qualitative evidence synthesis. *Journal of Clinical Nursing, 26*(5–6), 873–881.

Huang, M., Neveol, A., & Lu, Z. (2011). Recommending MeSH terms for annotating biomedical articles. *Journal of the American Medical Informatics Association, 18*(5), 660–667.

Iliou, C., Kalpakis, G., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2016). Hybrid focused crawling for homemade explosives discovery on surface and dark web. *Proceedings of the 11th international conference on availability, reliability and security (ARES)*.

Jones, R., Simonson, P., & Singleton, N. (2010). *Experiences of stigma – Everyday barriers for drug users and their families. London: UK Drug Policy Commission.* Retrieved from: http://www.ukdpc.org.uk/publications.shtml#Stigma_reports.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59–68.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands: Summary. Santa Monica, CA/Cambridge, UK: RAND Europe.* Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1607/RAND_RR1607.pdf.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. *European Journal of Criminology, 12*(2), 226–241.

Mackey, T. K., & Kalyanam, J. (2017). Detection of illicit online sales of fentanyls via Twitter. *F1000 Research, 6*, 1937.
Mackey, T. K., Kalyanam, J., Katsuki, T., & Lanckriet, G. (2017). Twitter-based detection of illegal online sale of prescription opioid. *American Journal of Public Health, 107*(12), 1910–1915.
Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society, 19*(1), 111.
Maheshram, Y., & Singhai, S. (2018). Survey paper on crypto currency bitcoin. *International Journal of Research in Science & Engineering, 4*(2).
Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs.* Springer.
Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics, 23*(2), 261–277.
Mays, N., Pope, C., & Popay, J. (2005). Systematically reviewing qualitative and quantitative evidence to inform management and policy-making in the health field. *Journal of Health Services Research & Policy, 10*(Suppl 1), 6–20.
Miller, P. G., & Sønderlund, A. L. (2010). Using the internet to research hidden populations of illicit drug users: a review. *Addiction, 105*, 1557–1567.
Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *The American Behavioral Scientist, 61*(11), 1427–1450.
Moncur, W., Grimani, A., Gavine, A., Stevens, R., Wells, S., Francis, M., & Leslie, A. (2019). The Illustrated Guide to Keeping Secrets Online. In. Report 19-030-01: CREST.
Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review, 27*(4), 237–254.
Mounteney, J., Oteo, A., & Griffiths, P. (2016). *The internet and drug markets: shining a light on these complex and dynamic systems. The internet and drug markets (European monitoring centre for drugs and drug addiction: insights 21)*. Luxembourg: Publications Office of the European Union13–17.
Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy, 63*, 101–110.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Accessed on 03/07/19 at: http://bitcoin.org/bitcoin.pdf.
Nurmi, J., Kaskela, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road. *Drug and Alcohol Dependence, 178*, 201–207.
OFcom. (2019). *Online Nation.* Retrieved from https://www.ofcom.org.uk/_data/assets/pdf_file/0025/149146/online-nation-report.pdf.
Paquet-Clouston, M., Décary-Hétu, D., & Morselli, C. (2018). Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy, 54*, 87–98.
Phelps, A., & Watt, A. (2014). I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation, 11*(4), 261–272.
Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., et al. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC methods programme. UK: University of Lancaster*.
Rhumorbarbe, D., Staehli, L., Broseus, J., Rossy, Q., & Esseiva, P. (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic Science International, 267*, 173–182.
Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019). BlackWidow: Monitoring the dark web for cyber security information. *Paper Proceedings of the 11th international conference on cyber conflict (CyCon)*.
Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Proceedings of the 2015 USENIX security symposium*.
Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation, 7*(17), 1–16.
Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology, 8*, 45.
Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *The International Journal of Drug Policy, 35*, 58.
UNODC. (2014). *Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies. United Nations Office on Drugs and Crime.* Retrieved from https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf.
Uutela, A. (2001). Drugs: Illicit use and prevention. In N. J. Smelser, & P. B. Baltes (Eds.). *International encyclopedia of the social & behavioral sciences* (pp. 3877–3881). Helsinki: National Public Health Institute.
van de Ven, K., & Koenraadt, R. (2017). Exploring the relationship between online buyers and sellers of image and performance enhancing drugs (IPEDs): Quality issues, trust and self-regulation. *The International Journal on Drug Policy, 50*, 48.
Van Hout, M. C., & Bingham, T. (2013a). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385–391.
Van Hout, M. C., & Bingham, T. (2013b). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*(6), 524–529.
Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183–189.
Walsh, D., & Downe, S. (2006). Appraising the quality of qualitative research. *Midwifery, 22*(2), 108–119.
Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism, 39*(3), 195–206.